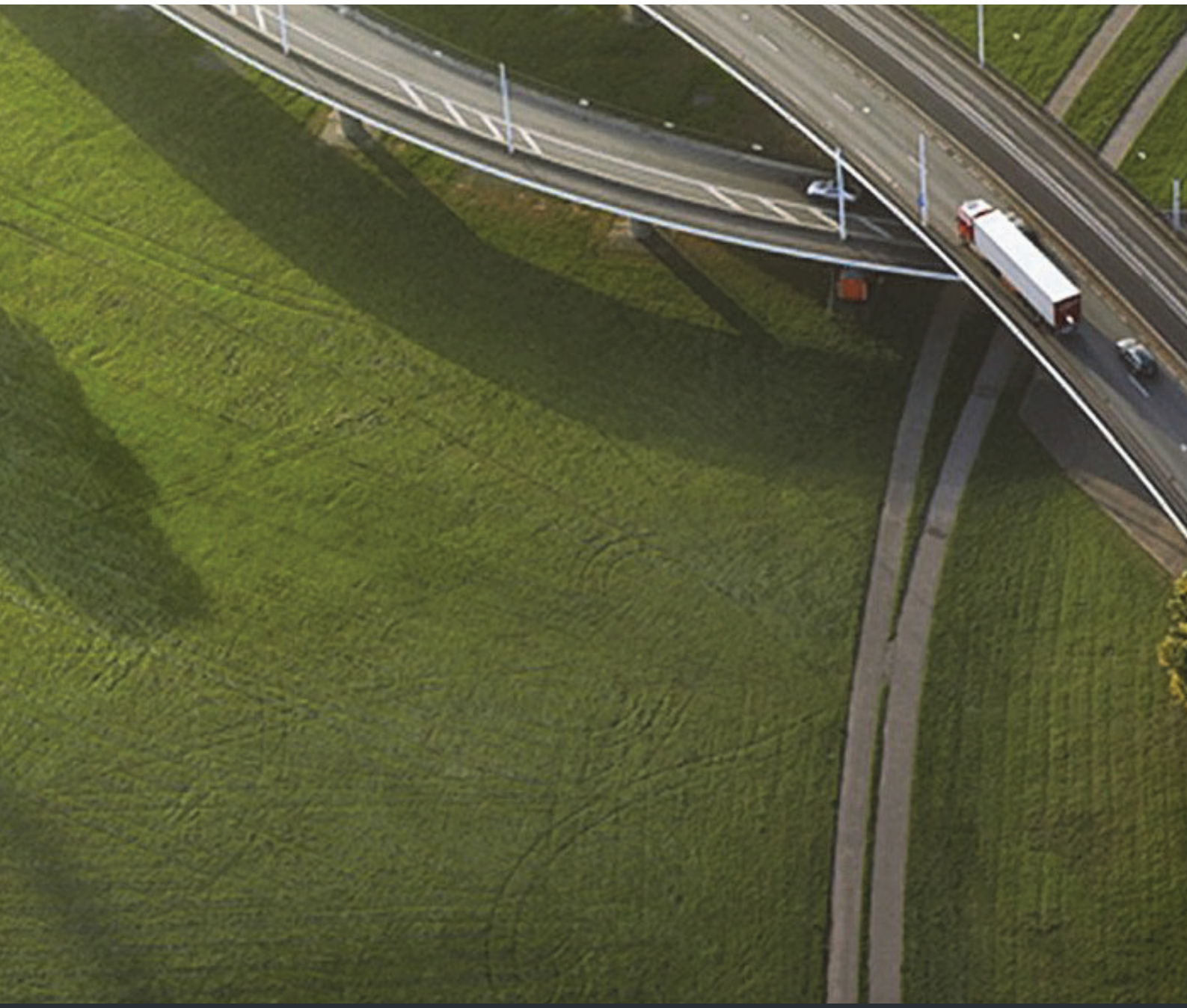
UNIFY Harmonize your enterprise



OpenScape Desk Phone IP openStage SIP V3R3 Security Checklist

Planning Guide

A31003-D3000-P100-01-76A9

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Copyright © Siemens Enterprise Communications GmbH & Co. KG. 10-2013
Hofmannstr. 51, 81379 Munich/Germany

All rights reserved.

Reference No.: A31003-D3000-P100-01-76A9

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.
An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Siemens Enterprise Communications GmbH & Co. KG.. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

unify.com

Contents

1 Introduction . . . 5
1.1 History of Change . . . 5
1.2 General Remarks . . . 5
1.3 Security Strategy for Unify Products . . . 6
1.4 Customer Deployment - Overview . . . 8

2 OpenStage Interfaces and Ports . . . 9

3 Phone Hardening Measures at a Glance . . . 10

4 Phone Hardening Measures . . . 12
4.1 Install latest (“Up-to-date”) OpenStage / Desk Phone IP Phone Software . . . 12
4.2 Secure Administration Access to the Phone . . . 12
4.2.1 Harden Local phone Admin Access . . . 13
4.2.2 Harden Local phone User Access . . . 14
4.2.3 Harden DLS Interface to the Phone . . . 15
4.2.4 Harden Software Deployment and File Download to the Phone . . . 17
4.3 Configure Password Policy and Passwords . . . 18
4.4 Authentication of phone at SIP Server . . . 19
4.5 Secure Signalling and Voice/Video Access to the Phone . . . 20
4.5.1 Harden Signalling to Secure Signalling . . . 20
4.5.2 Harden Phone to use Secure (Encrypted) Voice and Video . . . 22
4.6 Secure Interfaces and Services to the Phone . . . 23
4.6.1 PC Port . . . 23
4.6.2 OpenStage Manager Connection / CCE Interface . . . 23
4.6.3 USB Interface . . . 24
4.6.4 Remote Call Control (CSTA) . . . 25
4.6.5 Bluetooth Access . . . 26
4.6.6 LDAP . . . 27
4.7 Secure Access to Network (Use IEEE 802.1x Access Control) . . . 28
4.8 XML Applications . . . 29

5 Administration . . . 31
5.1 System Access . . . 31
5.1.1 Serial Interface Access . . . 31
5.2 Remote Administration . . . 31
5.3 Web Services . . . 32
5.4 Monitoring via SNMP . . . 32
5.5 Diagnostics . . . 33
5.6 SSH Interface . . . 34

6 Addendum . . . 36
6.1 Default Accounts . . . 36
6.2 Password and PIN Policies . . . 36
6.2.1 Password Policy supported by OpenStage and Desk Phone IP phones . . . 36
6.2.2 PW Policy agreed for customers deployment . . . 37
6.3 Certificate Handling . . . 39
6.3.1 Credentials used for Openstage and Desk Phone IP SIP V3R3 . . . 40
6.3.2 Setup Certificate Checking Policy . . . 41
6.4 Port Table . . . 42

6.5 References 42
Index 44

1 Introduction

1.1 History of Change

Date	Version	What
2013-09-20	0.1	Initial Draft
2013-10-14	0.2	Update with comments received. There are structural changes in some areas to better align with the SCL template
2013-10-23	1.0	Update with comments received. Added References into CLs. Changed Siemens to Unify

1.2 General Remarks

Information and communication and their seamless integration in “Unified Communications and Collaboration“ (UCC) are important, valuable assets forming the core parts of an enterprise business. These assets require every enterprise provide specific levels of protection, depending on individual requirements to availability, confidentiality, integrity and compliance for the communication system and IT infrastructure it utilizes.

Unify attempts to provide a common standard of features and settings of security parameters within delivered products. Beyond this, we generally recommend

- to adapt these default settings to the needs of the individual customer and the specific characteristic of the solution to be deployed
- to weigh the costs of implementing security measures against the risks of omitting a security measureand to “harden” the systems appropriately.

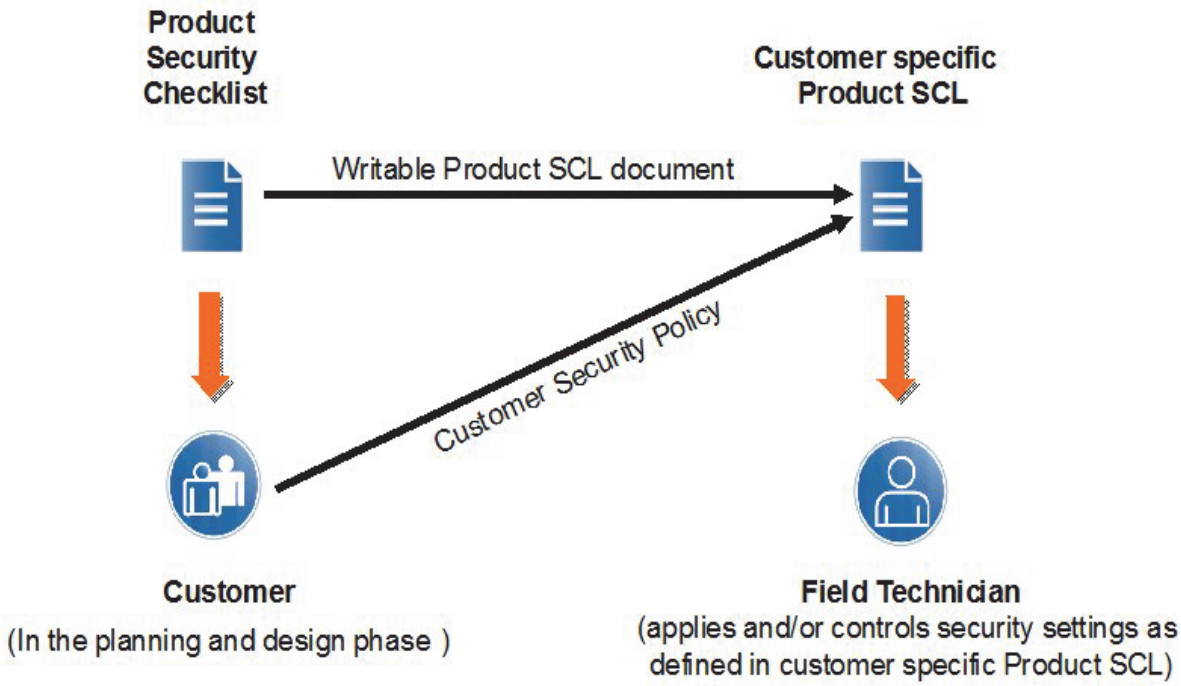
Product Security Checklists are published as a basis to support the customer and service department in both direct and indirect channels, as well as self-maintainers, to document security setting agreements and discussions.

The Security Checklists can be used for two purposes:

- **In the planning and design phase** of a particular customer project:
  Use the Product Security Checklists of every relevant product to evaluate, if all products that make part of the solution can be aligned with the customer’s security requirements – and document in the Checklist, how they can be aligned. The Product Security Checklist containing customer alignments can be identified as Customer specific Product Security Checklist.
  This ensures that security measures are appropriately considered and included in the Statement of Work to build the basis for the agreement between Unify and the customer: who will be responsible for the individual security measures:

  - During installation/setup of the solution
  - During operation
- **During installation and during major enhancements or software upgrade activities:**
  The Customer specific Product Security Checklists are used by a technician to apply and/or control the security settings of every individual product.

Figure: Usage of Security Checklists (SCL)


Product Security Checklist
Customer specific Product SCL
Writable Product SCL document
Customer Security Policy
Customer
(In the planning and design phase)
Field Technician
(applies and/or controls security settings as defined in customer specific Product SCL)

Update and Feedback

- By their nature, security-relevant topics are prone to continuous changes and updates. New findings, corrections and enhancements of this checklist are being included as soon as possible.
  Therefore, we recommend using always the latest version of the Security Checklists of the products that are part of your solution.
  They can be retrieved from the Unify partner portal http://www.unify.com/us/partners/partner-portal.aspx for the entire product .
- We encourage you to provide feedback in any cases of unclarity, or problems with the application of this checklist.
  Please contact the Openscape Baseline Security Office (obso@unify.com).

1.3 Security Strategy for Unify Products

Reliability and security is a key requirement for all products, services and solutions delivered by Unify. This requirement is supported by a comprehensive security software development lifecycle that applies to all new products or product versions being developed from design phase until end of life of the product.

Products of Unify are developed according to the Baseline Security Policy, which contains the technical guidelines for the secure development, release and sustaining of the company's products. It defines the fundamental measures for software security that are taken throughout the whole lifecycle of a product, from design phase until end of life:

Product planning and design:

Threat and Risk analysis (Theoretical Security Assessment) to determine the essential security requirements for the product.

Product development and test:

Penetration Tests (Practical Security Assessment) to discover implementation vulnerabilities and to verify the hardening of the default system configuration.

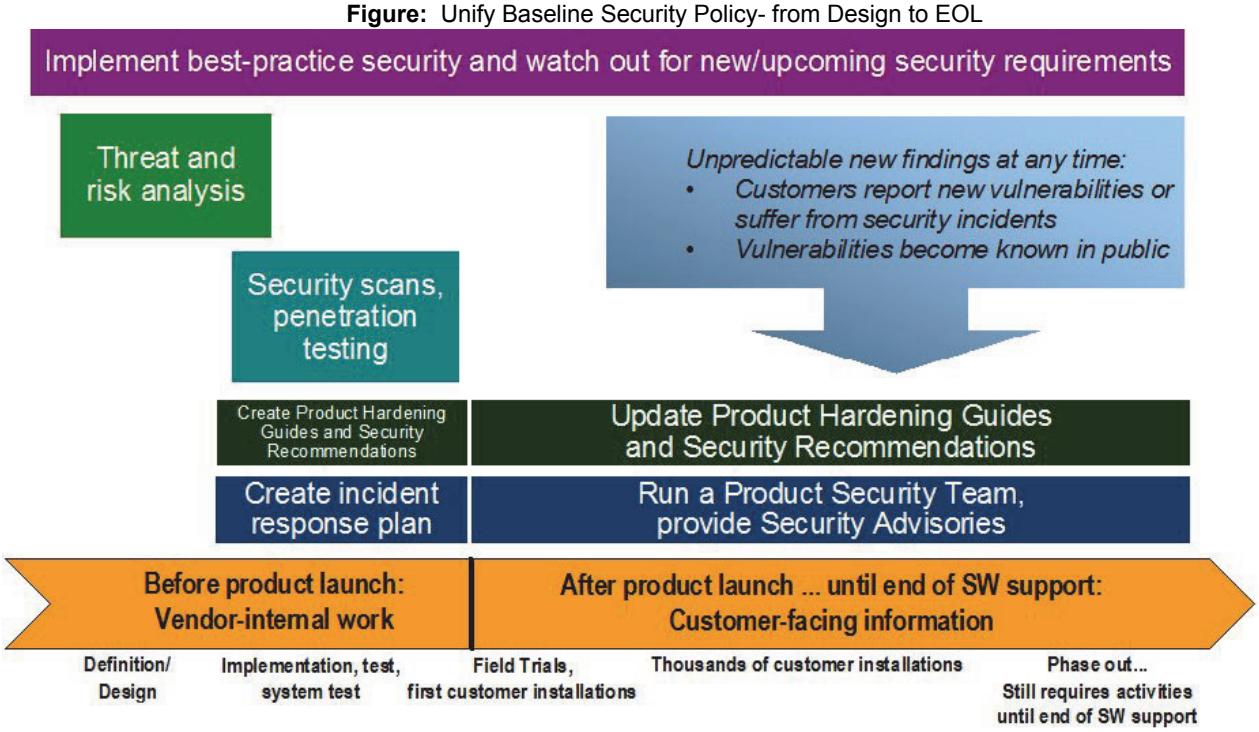
Installation and start of operation:

Hardening Guides (Security Checklist) to support the secure configuration of the product according to the individual customer's security policy.

Operation and maintenance:

Proactive Vulnerability Management to identify, analyse and resolve security vulnerabilities that emerge after products have been released, and to deliver guidance to customers how to mitigate or close these vulnerabilities.

Figure: Unify Baseline Security Policy- from Design to EOL


Implement best-practice security and watch out for new/upcoming security requirements
Threat and risk analysis
Unpredictable new findings at any time:
• Customers report new vulnerabilities or suffer from security incidents
• Vulnerabilities become known in public
Security scans, penetration testing
Create Product Hardening Guides and Security Recommendations
Update Product Hardening Guides and Security Recommendations
Create incident response plan
Run a Product Security Team, provide Security Advisories
Before product launch: Vendor-internal work
After product launch ... until end of SW support: Customer-facing information
Definition/ Design
Implementation, test, system test
Field Trials, first customer installations
Thousands of customer installations
Phase out... Still requires activities until end of SW support

For more information about the Unify product security strategy we refer to the relevant Security Policies [3], [4], [5].

As we at Unify define a secure product, our products are not secure, but - they can be installed, operated and maintained in a secure way. The level of the products security should be scheduled by the customer.

The necessary information for that is drawn up in the Product Security Checklist.

1.4 Customer Deployment - Overview

This Security Checklist covers the product and lists their security relevant topics and settings in a comprehensive form.

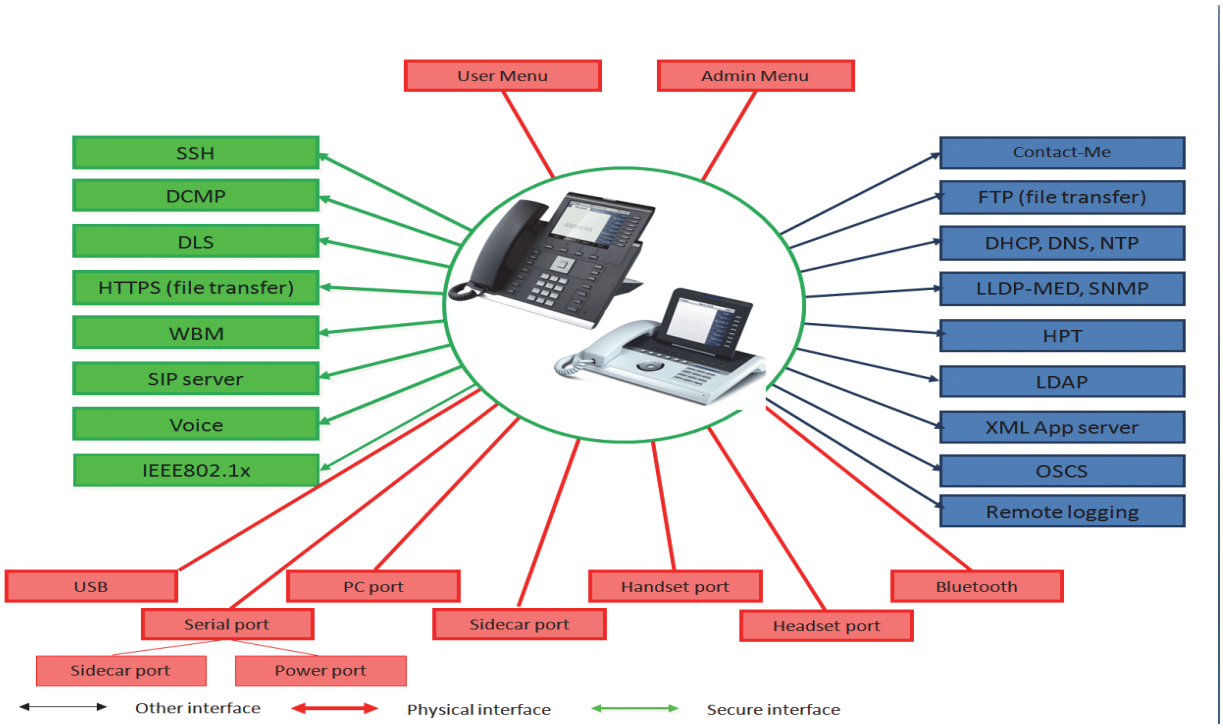
	Customer	Supplier
Company		
Name		
Address		
Telephone		
E-mail		
Covered Systems (e.g. System, SW version, devices, MAC/IP-addresses)		
Referenced Master Security Checklist	Version:	
	Date:	
General Remark		
Open issues to be resolved until		
Date		

2 OpenStage Interfaces and Ports

Considering hardening for OpenStage and Desk Phone IP SIP V3R3 all interfaces and ports have to be analysed.

The interfaces for OpenStage and Desk Phone IP SIP V3R3 phones are shown in a landscape diagram below. Complete information about used interfaces/IP ports is part of the release notes as well as from the Unify Partner Portal.

http://www.unify.com/us/partners/partner-portal.aspx



3 Phone Hardening Measures at a Glance

To improve the security on OpenStage and Desk Phone IP SIP V3R3 phone the following measures are recommended

(http://www.unify.com/us/partners/partner-portal.aspx

Latest Software

- Install latest (“Up-to-date”) Desk Phone IP 35G V3R2 phone software during initial startup phase. The software is ready to download from the partner portal Siemens Enterprise Business Area (https://www.siemens-enterprise.com/seba/default.aspx)

Phone Administration: local, WBM, DLS, serial port

- Secure local phone administration
  - Physical access, Phone lock
  - Set passwords & apply password policy (refer to main chapter Password and PIN Policies)
  - Lock-down configuration items via DLS, so that these are not changeable from the user account
- Hardening of web-based management
  - Set passwords & apply password policy (refer to main chapter Password and PIN Policies)
  - Deactivate if not used
  - Install customer individual WBM certificate and private key
- Hardening of DLS interface
  - Set communication between phone and DLS to “secure mode”
  - Use HTTPS server instead of FTP server and as an alternative to the DLS for file and software deployment
  - Certificates (CA & client) must be downloaded and the certificate policy set

Set passwords and apply password policy (Password and PIN Policies)

- Apply password policy as recommended
- Set minimum password length
- Modify default admin password
- Set user password

Install certificates and configure secure calls

- Use of OCSP to verify validity of certificates and set a proper policy
- Install TLS certificates and private keys as well as CA certificates
- Enable SIP Signalling encryption
- Enable SIP Payload Encryption and disable video calls

Enable IEEE 802.1x in the network and at the phone by installing the appropriate certifications

Use digest authentication

Interfaces / Ports

- Disable factory reset via hooded claw
- Enable remote trace only when needed
- Enable PC port only if really required
- Enable SSH access only if really required
- Disable OSCS / Phone Manager access if not required?
- Enable CSTA/ CTI access only if really required?
- Disable USB access if not needed?
- Disable WBM access if not needed?
- Enable SNMP only if required?
- Disable BlueTooth if not needed?
- Use TLS encryption for LDAP

XML Applications / Send URL?

- Do not configure XML applications if not needed?
- Use HTTPS for XML and Send URL applications
- Deploy Server CA Certificates and enable checking

The recommended measures are listed in the following chapters.

4 Phone Hardening Measures

4.1 Install latest (“Up-to-date”) OpenStage / Desk Phone IP Phone Software

The latest (“up-to-date”) released OpenStage /Desk Phone IP SIP V3R3 software version should be installed during initial setup. The software is ready to download from the Unify Partner Porta (http://www.unify.com/us/partners/partner-portal.aspx).

For improved security it is recommended to perform the initial configuration of OpenStage phones in a separate staging lab.

Table: Phone Software Version

CL - ’SW status	
Measures	Up-to-date SW installed for OpenStage / Desk Phone IP
References	See Phone Administration Manual chapter on Transferring Phone Software -> Download / Update Phone Software
Can be done via	Local Administration, WBM, DLS
Needed Access Rights	Admin Access
Executed	Yes ☐ No: ☐
Phone Types	
Customer Comments and Reasons	

4.2 Secure Administration Access to the Phone

The administration of the phone has to be protected from unauthorized access. There are several measures to facilitate a secure local phone administration, the hardening of web-based management and the hardening of DLS interface.

Fixed passwords are a serious security risk, and the Password and PIN policy in Chap. Password and PIN Policies is strongly recommended. The access to the phone is possible on two levels: Admin and User. Each level has its own password policy and password. Separate passwords should be used for Admin and User access.

4.2.1 Harden Local phone Admin Access

Table: Harden Local phone Admin Access

CL-Secure Admin Access	
Measures	• Setup the password policy for Admin password • Set a secure Admin password for each phone • If not needed, disable local administration access at the phone. This can only be done using DLS • Disable Hooded Claw for Factory reset
References	See Chapter Password and PIN Policiesfor setting Password policy See Phone Administration Manual chapter on Security -> Password Policy
Can be done	
Needed Access Rights	Admin Access
Executed: Setup Generic Admin Password Policy	Yes ☐ No: ☐
Set Secure Admin password	Yes ☐ No: ☐
Setup Admin Password Policy	Yes ☐ No: ☐
Disable Local Admin Access	Yes ☐ No: ☐
Disable Hooded Claw for Factory Reset	Yes ☐ No: ☐
Customer Comments and Reasons	

4.2.2 Harden Local phone User Access

In addition to setting an individual secure password for each phone the following can be done to harden user access to the phone.

- Where phones should only be used by specific users – for example for phones in secure areas where visitors are not allowed access to use the phone, or in public areas where public use of the phone is not allowed then the Phone Lock feature should be turned on. A valid User password is needed for this feature.
  Emergency calls are possible while the phone is locked, but Users will need to unlock the phone to make regular calls and gain access to user data on the phone – for example call log or directory;
- To prevent users making changes to configuration items the User access can be blocked at the following levels:
  - Particular configuration items can be locked down by configuration of the data constraints in the DLS
  - User access to the User menus can be disabled. The user can still set forwarding and configure the programmable FPK keys, but access to individual user settings are disabled

  INFO: If the local user access is disabled then the phonelock feature will not work.

- If the customer's security policy is to prevent access to information about the phone setup such as the IP address being used then access to the diagnostic data should be disabled

Table: Harden Local phone User Access

CL-Secure User Access	
Measures	• Setup the password policy for User password • Set an individual User password for each phone • Set Phone Lock ON • Lock Down particular data items by configuration at DLS • Disable User Access to configuration menus • Disable access to diagnostic data if needed to comply with customer's security policy
References	See Chapter Password and PIN Policiesfor setting Password policy. See Phone Administration Manual chapter on Security -> Password Policy
Can be done	
Needed Access Rights	Admin Access
Executed Setup Generic User Password Policy	Yes ☐ No: ☐

CL-Secure User Access	
Setup User Password Policy	Yes ☐ No: ☐
Secure User password Set	Yes ☐ No: ☐
Set Phone Lock ON	Yes ☐ No: ☐
Lock Down required configuration data	Yes ☐ No: ☐
Disable User Access to Diagnostic Data	Yes ☐ No: ☐
Customer Comments and Reasons	

4.2.3 Harden DLS Interface to the Phone

The communication between DLS and Phone can be configured in default mode. In the default mode the phone recognizes the DLS because it knows the DLS IP address. There is no authentication between Phone and DLS.

- When the DLS IP Address is provided by the DHCP Server, service access with a second DLS is not possible because DLS IP Address is supplied only by DHCP.
- In the case where the DLS IP Address is not provided by the DHCP Server, a second DLS (even a threatened one) could take over the control of the phone.

If the communication between DLS and phone is configured in secure mode, they authenticate via HTTPS mutual authentication. Now a second DLS only can get read/write access to the phone if it knows the customer specific credentials.

- Independently of the usage of a DHCP Server, a service access with a second DLS is possible, if the second DLS uses the customer specific credentials for authentication. The phone itself always contacts the first DLS.

In all cases the security of the DHCP Server access is in customer's hand. His network should be able to recognize a second (may be threatened) DHCP server, e.g. by using an IDS system.

Setting communication between phone and DLS to “secure mode”

"Secure mode" offers mutual authentication between DLS and the phone. The connection between DLS and phone will be established, if DLS has successfully authenticated the phone and vice versa. Secure mode with or without PIN (Personal Identification Number) will be set by the DLS. The PIN has to be inputted at the phone when requested. “Secure mode with PIN” protects the transfer of the key material and should be preferred. Us-age of Secure mode without PIN may offer an attacker to capture the key material and may get non-authorized access to the DLS and phone.

Prerequisites for the usage of the secure mode are the following:

- Customer specific key material has to be created, e.g. with customers own CA or with openSSL or other tool. Provided by customer.
- The key material is distributed by DLS to phones in default mode (in customer network or preconfigured). The distribution of keys and certificates via DLS (Deployment Service) is depicted in the Deployment Service Admin Guide, chapter " Automatic Certificate Deployment"
- Both, phones as well as DLS have to be set to "secure mode" How to configure the secure mode for phone is described in: "IP Device Configu-ration"

Table: Secure Communication with DLS Servert

CL-Secure DLS Access	
Measures	• If using Default mode ensure that the DLS address is provided by the DHCP • For improved security use secure mode between DLS and Phone
References	See Phone Administration Manual chapters on Vendor Spe-cific: VLAN Discovery and DLS Address and How to Use Option #43 “Vendor Specific” See DLS manual Configuration & Update Service (DLS)
Can be done via	
Needed Access Rights	Administrator Access
Executed Provide DLS IP address from DHCP	Yes ☐ No: ☐
Setup Secure mode for DLS –Phone communica-tions	Yes ☐ No ☐
Customer Comments and Reasons	

4.2.4 Harden Software Deployment and File Download to the Phone

To provide a secure file download for the files (for example ringer files) and software updates loaded onto the phone HTTPS should be used. A separate HTTPS download server will be needed.

Authentication of the HTTPS server at the phone is also needed and this can be setup by loading the HTTPS server CA certificate into the phone and configuring the authentication policy. Mutual authentication is possible when both the HTTPS Server CA certificate and the Phone HTTPS client certificate are loaded in the phone.

Table: Secure Software Deployment and File download

CL-Secure Software Deployment and File download	
Measures	• Configure Download of Software Deployment and files such as screensavers or ringtones to use HTTPS ? • Install the HTTPS Server CA certificate and a HTTPS phone client certificate in the phone? • The HTTPS certificate policy needs to be set to Trusted or Full? • OCSP checking of the certificate will ensure that the certificate from the HTTPS server has not been revoked
References	See Chapter Password and PIN Policiesfor Certificate Handling. See Phone Administration Manual chapters on Security -> Certificate Policy and Transferring Phone Software -> Download / Update Phone Software See DLS manual Configuration & Update Service (DLS) for installing certificates
Needed Access Rights	Admin Access
Executed Configure Phones to use HTTPS for software and file download	Yes ☐ No: ☐
Install HTTPS certificates on the phone:	Yes ☐ No: ☐
Configure Secure File Transfer certificate policy:?	Yes ☐ No: ☐

CL-Secure Software Deployment and File download	
Configure OCSP checking	Yes ☐ No: ☐
Customer Comments and Reasons	

4.3 Configure Password Policy and Passwords

The OpenStage and Desk Phone IP phones are delivered with default passwords and password policy. These must be changed to the customer specific passwords and password policy. The recommended password and PIN policy is in chapter Password and PIN Policies.

Table: Secure Software Deployment and File download

CL-Secure passwords	
Measures	• Set the Generic Password Policy? • Set the Admin Access password policy • Set the User Access password policy • Set secure Admin password • Set individual secure User password for each phone
References	See Chapter Password and PIN Policiesfor password and PIN policy. See Phone Administration Manual chapter on Security -> Password Policy
Needed Access Rights	Admin Access
Executed Setup Generic Password Policy	Yes ☐ No: ☐
Setup AdminPassword Policy	Yes ☐ No: ☐
Setup User Password Policy	Yes ☐ No: ☐

CL-Secure passwords	
Set Secure Admin password	Yes ☐ No: ☐
Set Secure User passwords for phones	Yes ☐ No: ☐
Customer Comments and Reasons If some measures are not executed then please explain here.	

4.4 Authentication of phone at SIP Server

To ensure that only authorized phones contact the SIP Server Unify provides the state-of –the-art Digest Authentication mechanism-

The Digest Authentication uses a Challenge Response Algorithm. It is uses a userID – which can be the phone number – and a password. The SIP server sends a Challenge and the phone responds with its password.

Digest Authentication can be used without Secure signalling over TLS – the password is transmitted in a secure format, but use of TLS signalling is strongly recommended to provide an overall security for the signalling. Use of TLS will also allow authentication by the phone of the SIP Server – see Chapter Harden Signalling to Secure Signalling.

The Digest Authentication must be configured on the SIP Server before setting up the phone. Please see the Security Check List for the SIP server.

Table: Digest Authentication

CL- Secure Phone Authentication on SIP Server	
Measures	Setup Digest Authentication User-ID and Password
References	See Phone Administration Manual chapter on System Settings -> SIP registration
Can be done via	
Needed Access Rights	Administrator
Executed Set SIP Authentication UserID and Password in the phone	Yes ☐ No: ☐
Customer Comments and Reasons	

4.5 Secure Signalling and Voice/Video Access to the Phone

To give privacy for Voice and Video connections, the Openstage and Desk Phone IP phones should use TLS for the signalling and Secure RTP for the voice and video connections.

4.5.1 Harden Signalling to Secure Signalling

To provide a secure signalling mechanism TLS signalling should be used.

- Configure use of TLS on the SIP server and install server certificates.
- Configure TLS on the phone – the port will need to be set to 5061.

In addition to using TLS signalling, authentication of the server by the phone can be done by validating the Server certificate sent by the SIP server.

- Install the SIP Server CA certificate on the phone using DLS.
- Configure the TLS certificate validation policy to trusted or full – full is recommended.
- Configure OCSP checking to allow revocation checking of the SIP server certificate.

It should be noted that if the Backup / Dual registration mode is used as part of survivability setup, the phone only supports TLS on the connection to the primary SIP server. The connection used for the backup/dual registration is only possible using UDP or TCP not TLS. To avoid this vulnerability the use of DNS-SRV is recommended for survivability setup. To avoid unplanned use of UDP/TCP when using TLS connections the Backup Proxy Address should be configured as 0.0.0.0. ?

Table: SIP Secure Signalling

CL-SIP Secure Signalling	
Measures	• Configure use of TLS on the SIP server and install server certificates • Configure TLS on the phone – the port will need to be set to 5061 • Install the SIP Server CA certificate on the phone using DLS • Configure the TLS certificate validation policy to trusted or full – full is recommended • Configure OCSP checking to allow revocation checking of the SIP server certificate • Configure the Backup proxy address 0.0.0.0 Apply password policy (user and administrator)
References	See Chapter Certificate Handlingfor Certificate Handling. See Phone Adminstration Manual chapter on Security -> Certificate Policy See DLS manual Configuration & Update Service (DLS) for installing certificates See Phone Administration Manual chapter on System Settings -> SIP Addresses and Ports
Can be done via	
Needed Access Rights	Administrator
Executed Set Signalling Transport to TLS	Yes: ☐ No: ☐
Set Port for Signalling to value 5061	Yes: ☐ No: ☐
Install TLS certificate on the phone using DLS:	Yes: ☐ No: ☐
Configure Secure SIP Server certificate policy	Yes: ☐ No: ☐
Configure OCSP check	Yes: ☐ No: ☐

CL-SIP Secure Signalling	
Configure Backup Proxy address to 0.0.0.0	Yes: ☐ No: ☐
Customer Comments and Reasons. If some measures are not executed then please explain here.	

4.5.2 Harden Phone to use Secure (Encrypted) Voice and Video

To provide secure encrypted communication for voice and video calls, secure calls and the key exchange protocol (SDES or MIKEY) must be configured. Secure Video calls are only possible using SDES.

Secure signalling must be setup before doing the setup for secure voice and video. (see section Harden Signalling to Secure Signalling)

Table: SIP Secure Signalling

CL-Secure Calls	
Measures	• Configure Secure Calls • Configure Key Exchange protocol (SDES or MIKEY) – must use SDES if using video calls. • If using SDES configure the parameters for SDES
References	See Phone Administration Manual chapter on Security -> Speech Encryption
Can be done via	
Needed Access Rights	Administrator
Executed Configure Secure Calls (the single setting applies to both voice and video calls)	Yes: ☐ No: ☐
Configure SRTP type (Mikey or SDES)	Yes: ☐ No: ☐
If SDES selected, configure SDES parameters	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.6 Secure Interfaces and Services to the Phone

To allow easy initial use of Openstage and Desk Phone IP phones, the majority of services and interfaces are enabled by default. To harden the phone, services and interfaces not used should be disabled. Also where a more secure protocol is available for a service then that should be configured, for example use TLS instead of UDP or TCP.

4.6.1 PC Port

The PC port allows a LAN cable to be connected directly between the phone and an adjacent PC, thereby using the same LAN connection for both PC and Phone at the desk. To prevent unauthorised access to the network using the PC port on the phone, the port should be disabled if not needed

The default setting for the PC port is disabled, but it should be checked that PC port is disabled on phones which do not need a local PC connection

Table: SIP Secure Signalling

CL-PC Port	
Measures	• Disable PC Port
References	See Phone Administration Manual chapter on System Settings -> SIP Addresses and Ports
Can be done via	
Needed Access Rights	Administrator
Executed Disable PC Port if not needed by user	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.6.2 OpenStage Manager Connection / CCE Interface

On OpenStage 60 , OpenStage80 and Desk Phone IP 55G phones the OpenStage Manager PC application is used for customisation of the phone (e.g. ringtones, key programming). To prevent unauthorised access to the phone, if the Openstage Manager application is not used then the CCE interface should be disabled.

INFO: This port is also used by the HPT tool, and disabling the port will prevent use of the HPT tool.

Table: SIP Secure Signalling

CL-Openstage Manager Connection	
Measures	• Disable CCE access
References	See Phone Administration Manual chapter on Security -> Access Control
Can be done via	
Needed Access Rights	Administrator
Executed Disable CCE access if not needed by user for Open-stage Manager application	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.6.3 USB Interface

On OpenStage 60 , OpenStage 80 and Desk Phone P55G phones there is a USB interface for connection of video camera or USB memory stick. To prevent unauthorised access to the phone, if USB devices (camera/ memory stick) are not used then the USB interface should be disabled.

To prevent unauthorised transfer of a users data off the phone onto a memory stick , but still have the USB port available for use by USB camera, there is the option to disable access for a USB Backup / restore

Table: SIP Secure Signalling

CL-USB port	
Measures	• Disable USB interface • If USB interface is enabled – disable USB backup/restore
References	See Phone Administration Manual chapter on Feature Access
Can be done via	
Needed Access Rights	Administrator
Executed Disable USB interface if not needed by user for USB camera or USB memory stick	Yes: ☐ No: ☐

CL-USB port	
Disable USB Backup / Restore	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.6.4 Remote Call Control (CSTA)

Call Setup is possible by remote CTI clients running on a PC or server. The call control is performed using CSTA and uaCSTA protocol in SIP messages from the SIP server.

It is possible for this to be used in a malicious way and the service should only be enabled where needed. A CTI service allowed/not allowed setting is available at Admin level to control this

When the CTI service is allowed then the user can choose to use auto answer or not. Setting auto answer to off will prevent unwanted automatic answering of calls setup by a remote client - for example for phones in conference rooms or public areas. When Auto Answer is configured off then each call will be presented to the user, and the user must accept the call before it is answered.

Table: SIP Secure Signalling

CL-SIP Secure Signal-ling	
Measures	• Set CTI Service to Disallow if not needed • Set Auto Answer to No if not needed
References	See Phone Administration Manual chapter on Feature Access? See Phone User Guide chapter on Enhanced phone functions -> incoming calls -> CTI calls
Can be done via	
Needed Access Rights	Administrator
Executed If CSTA feature is not used then set CTI control to disallow?	Yes: ☐ No: ☐

CL-SIP Secure Signal-ling	
If CTI is allowed and Auto Answer is not wanted or used then set Auto Answer to No	Yes: ☐ No: ☐
Customer Comments and Reasons. If some mea-sures are not executed then please explain here.	

4.6.5 Bluetooth Access

On OpenStage 60 and OpenStage 80 phones Bluetooth is available and allows use of Bluetooth headsets or transfer of contact information (vcard).

- If Bluetooth is not used then it should be disabled
- If Bluetooth is enabled then the method of pairing can be set to be automatic or needing a prompt. To ensure that the user is aware when another device is paired with their phone and to prevent unauthorised pairing the pairing method should be set to “prompt” and the pairing PIN must be set by the user.?
- If Bluetooth is enabled then to reduce possibility of unauthorised pairing attempts the discoverable parameter should only be set to YES by the user when needed for pairing.

Table: SIP Secure Signalling

CL-Bluetooth	
Measures	• Disable Bluetooth if not used. • If Bluetooth is enabled, inform user to set pairing mode to prompt and the configure a pairing PIN. • If Bluetooth is enabled, inform user to set Discoverable to NO except when needed for setup of pairing.
References	See Phone Administration Manual chapter on Bluetooth?. See Phone User Guide chapter on Individual phone configu-ration -> Bluetooth
Can be done via	
Needed Access Rights	Administrator, User
Executed If Bluetooth is not needed then disable in Admin me	Yes: ☐ No: ☐

CL-Bluetooth	
If Bluetooth is enabled then inform user to set pairing mode to prompt and to configure the pairing PIN	Yes: ☐ No: ☐
If Bluetooth is enabled then inform user to set Discoverable to NO except when needed for setup of pairing.	Yes: ☐ No: ☐
Customer Comments and Reasons. If some measures are not executed then please explain here.	

4.6.6 LDAP

To harden access to the LDAP server

- simple authentication should be used with a userid and password configured in the phone
- encrypted LDAP using TLS should be used to prevent data exchanged during an LDAP query being visible on the LAN.

Note that only encryption is used; authentication of the LDAP server is not available in V3R3

Table: SIP Secure Signalling

CL-Secure phone access to LDAP Server	
Measures	• Configure simple authentication with userid and password • Configure TLS as transport protocol
References	See Phone Administration Manual chapter on Corporate Phonebook: Directory Settings -> LDAP
Can be done via	
Needed Access Rights	Administrator
Executed Configure Simple Authentication and set the LDAP UserID and Password in the phone	Yes: ☐ No: ☐

CL-Secure phone access to LDAP Server	
Set LDAP Transport to use TLS	Yes: ☐ No: ☐
Customer Comments and Reasons. If some measures are not executed then please explain here.	

4.7 Secure Access to Network (Use IEEE 802.1x Access Control)

The customer has the option to enable IEEE 802.1x in the network and at the phone by installing the appropriate certificates. This should be done in a secure “staging” area.

Support of IEEE 802.1x provides means of authenticating and authorizing a device attached to local area networks. For details and further information please refer to

http://wiki.unify.com/images/a/ae/DLS_Certificate_Management_for_802_1x.pdf

http://wiki.unify.com/index.php/VoIP_Security

and

http://wiki.unify.com/images/2/23/IEEE_802.1X_Configuration_Management.pdf

Table: IEEE 902.1x enabling

CL- Enable 802.1x	
Measures	• Configure 802.1x options • Install certificates onto the phone • Check that 802.1x certificate policy is trusted • Set MSCHAP-ID and password for PEAP mode
References	
Can be done via	DLS and enabling network for 802.1x (external switch configuration)
Needed Access Rights	Administrator
Executed Configure 802.1x options	Yes: ☐ No: ☐
Load 802.1x phone Client certificate onto the phone for EAP-TLS mode	Yes: ☐ No: ☐

CL- Enable 802.1x	
Load RADIUS server CA certificate onto the phone	Yes: ☐ No: ☐
Load RADIUS server CA certificate onto the phone	Yes: ☐ No: ☐
Set MSCHAP-Identity and Password for PEAP mod	Yes: ☐ No: ☐
Customer Comments and Reasons	

4.8 XML Applications

An XML Application runs on a remote server and provides a mechanism for the application to provide information and interact with the phone user using the phone screen. This is done using two mechanisms:?

- HTTP/HTTPS requests from the phone to the server with the response from the server providing information to be displayed.
- A PUSH mechanism where the XML Application pushes information onto the display of the phone. ?

Where XML applications are used on the OpenStage / Desk Phone IP then the setup of the XML application should be hardened by using HTTPS for the protocol and using certificate checking at the phone for authenticcation of the XML application server. To avoid DNS Spoofing the XML servers should be configured using IP addresses instead of host names.?

The Push mechanism can be mis-used, For a PUSH command to be accepted by the phone the XML Application has to be configured in the phone. To prevent unauthorised PUSH commands, if an XML application is not used on a phone then remove all configuration for that XML application to prevent unauthorised use and access to the phone.

Table: IEEE 902.1x enabling

CL- XML Application	
Measures	• Harden XML Application: – configure to use HTTPS – Install the ServerCA certificate for the XML application server – Set the XML certificate authentication policy to Trusted or Full – Enable OCSP checking • Delete XML Application configuration for XML Applications that are not needed by user.
References	See Phone Administration Manual chapter on Applications
Can be done via	
Needed Access Rights	Administrator
Executed	
Check XML applications configured on the phone and delete those not needed by the user.	Yes: ☐ No: ☐
For needed XML Applications	
Set protocol to HTTPS	Yes: ☐ No: ☐
Install Server CA certificate	Yes: ☐ No: ☐
Set XML application certificate policy to Trusted or Full:	Yes: ☐ No: ☐
Enable OCSP checking:	Yes: ☐ No: ☐
Customer Comments and Reasons. If some measures are not executed then please explain here	

5 Administration

5.1 System Access

Access to the administration of the phone has to be protected from unauthorised access. Access to the configuration of the phone is available two levels:

- User level access – see chapter "Harden Local phone User Access" for details how to harden the user access
- Admin level access – see chapter "Harden Local phone Admin Access" for details how to harden the admin access

5.1.1 Serial Interface Access

Access at a Linux level is possible using the serial interface with the special serial interface adaptor. To prevent unauthorised access this interface should be set to unavailable.

Table: Serial Interface Access

SCL- Serial Interface Access	
Measures	Set serial interface to Unavailable
References	See Phone Administration Manual chapter on Security Access Control
Can be done via	
Needed Access Rights	Administrator
Executed Set Serial Port access to unavailable:	Yes ☐ No: ☐
Customer Comments and Reasons	

5.2 Remote Administration

The Remote administration access must be hardened:

- DLS - see chapter Harden DLS Interface to the Phone
- Web Based Management. – see chapter Web Services

5.3 Web Services

Web services are provided on the phone to provide access to User and Admin configuration menus for use by web-based clients.

Access is only available using HTTPS. Attempts to access using the standard HTTP port are automatically redirected to HTTPS.

On delivery a default Web Server certificate is provided on the phone for this port. This must be replaced with a customer generated certificate.

The WBM access uses the same User and Admin passwords to restrict access to authorised users. Secure passwords must be set as in checklist chapters Harden Local phone User Accessand Harden Local phone Admin Access.?

To prevent unauthorised access via WEB browser and to reduce the probability of security vulnerabilities via the WEB browser, the WBM access should be disabled if WBM is not used?

Table: Web Access

CL- Web Access	
Measures	• Disable WBM access • Install Customer generated Web Server Certificate
References	See Phone Administration Manual chapter on Security Access Control? See DLS manual Configuration & Update Service (DLS) for installing certificates
Can be done via	
Needed Access Rights	Administrator
Executed Disable WBM access if not needed	Yes ☐ No: ☐
Install Web Server Certificate if Web Access is used	Yes ☐ No: ☐
Customer Comments and Reasons	

5.4 Monitoring via SNMP

The OpenStage and Desk Phone IP Phones use SNMP V1:

- to send traps to the SNMP Server for maintenance and QDC data
- for query of the phone MIB

A community string is available in SNMP V1 which is comparable with a userid or a password that allows access to read the MIBs on the phone. This must be set to allow access for SNMP query.

Similarly, servers receiving the Traps also make use of a community string . These are configured separately for traps and diagnostic traps (QDC data) in the phone.

As the community strings are transmitted in clear text they can be eavesdropped easily.

If SNMP is not used then to prevent unauthorised access to information SNMP should be disabled.

Table: Digest Authentication

CL- SNMP Access	
Measures	• Disable SNMP if not used. • If SNMP is used then Set the snmp community strings for query, trap and diagnostic trap (QDC).
References	See Phone Administration Manual chapter on IP Network Parameter -> SNMP
Can be done via	
Needed Access Rights	Administrator
Executed Disable SNMP if not used :	Yes ☐ No: ☐
Set SNMP Community Strings (Query/ Trap / Diagnostics)	Yes ☐ No: ☐
Customer Comments and Reasons	

5.5 Diagnostics

Trace data logging can be done either locally on the phone or to a remote server. The remote trace is done using the standard remote syslog function. This is transmitted in clear text and to prevent unwanted disclosure of information:

- Disable Remote trace if not needed
- Enable the Remote Trace User Notification function.

Remote diagnostic access is available using the HPT tool. Access for the HPT tool is allowed when a valid dongle file is downloaded onto the phone. To prevent unwanted access the HPT access should be disabled. This will delete the dongle file on the phone. This needs to be done after each diagnostic session where HPT is used.

Table: Diagnostic Access

CL-Diagnostic Access	
Measures	• Disable the remote trace facility (only needed for debug/ service fault finding) • Enable the Remote Trace User Notification function. • Disable the HPT access
References	See Phone Administration Manual chapter on Diagnostics -> Remote Tracing – Syslog, and Diagnostics-> HPT Interface
Can be done via	
Needed Access Rights	Administrator
Executed Set remote trace status to OFF	Yes: ☐ No: ☐
Set remote trace user Notification to ON:	Yes: ☐ No: ☐
Disable HPT to remove Dongle file from phone	Yes: ☐ No: ☐
Customer Comments and Reasons	

5.6 SSH Interface

The Secure Shell interface is reserved for technical specialists. **It is deactivated by default and can be enabled by the Admin user via WBM or DLS for each access.** It is enabled for a limited period of time only, and a password is set for the access. A different password should be used for each access. To prevent all access via secure shell the secure shell allowed can be disabled. This is done via DLS.

Table: SSH Interface Access

CL- SSH Interface Access	
Measures	Disable SSH Interface Access using DLS
References	See Phone Administration Manual chapter on SSH – Secure Shell Access
Can be done via	DLS
Needed Access Rights	Administrator

CL- SSH Interface Access	
Executed Set secure shell allowed to OFF (via DLS only):?	Yes ☐ No: ☐
Customer Comments and Reasons	

6 Addendum

6.1 Default Accounts

There are two access levels available on the phone. These are fixed as User and Admin and cannot be changed. Each access level has its own password and password policy.

6.2 Password and PIN Policies

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. OpenStage and Desk Phone IP SIP V3R3 technically supports the password policies depicted in chapter Password Policy supported by OpenStage and Desk Phone IP phones. For every password rule, a default value and a range of values that can be configured for that rule are given. If the default values don't fit with the customer's password policy, the values the customer wants to be configured shall be depicted in chapter PW Policy agreed for customers deployment.

6.2.1 Password Policy supported by OpenStage and Desk Phone IP phones

# Recommended Setting	Password policy of OpenStage and Desk Phone SIP V3R3	Default value (range of possible values)		Recommended Settings	Recommended Settings
		Password	PIN *	Password	PIN*
1	Minimal PW Length	6 (6 - 24)	6(6-24)	8	6
3	Minimal number of upper case letters	0 (0 – 24)	-	1	-
4	Minimal number of lower case letters	0 (0 – 24)	-	1	-
5	Minimal number of numerals	0(0 – 24)	(length)	1	-
6	Minimal number of special characters	0 (0 – 24)	-	1	-
7	Maximal number of repeated characters	0 (0 – 24)	0 (0 – 24)	3	3
8	Minimum character count for changed characters	0(0-24)	0 (0-24)	2	2
9	Password History	0 (0-99)	0(0-99)	5	5

# Recommended Setting	Password policy of OpenStage and Desk Phone SIP V3R3	Default value (range of possible values)		Recommended Settings	Recommended Settings
		Password	PIN *	Password	PIN*
10	Number of days password is kept in history	180 (1 – 999)	180 (1 – 999)	180	180
11	Maximum password age in days	0(0-99)	0 (0-99)	90	90
12	Minimum password age in hours	0 (0-24)	0 (0-24)	1	1
13	Notification before password expiration in days	0 (0-99)	0 (0-99)	4	4
14	Password change requires knowledge of old password	True	True	Not configurable	Not configurable
15	Force change default passwords/PINs after the first use	False	False	Can be set = true when PW is changed from DLS	Can be set = true when PW is changed from DLS
16	Maximum number of erroneous login attempts	0 (0=infinite, 2 – 5)	0 (0=infinite, 2 – 5)	5	5
17	Account lockout duration in minutes	0 (0 – 99)	0 (0 – 99)		
18	Automatic logoff after not used period in minutes	2 (1- 5)	2 (1- 5)	2	2

*OpenStage and Desk Phone IP Phones have a single configuration for both passwords and PINs. A PIN is a numeric only password and will use the same policy as configured for a password where possible.

6.2.2 PW Policy agreed for customers deployment

These are the customer PW/PIN rules for the PW Policy on OpenStage and Desk Phone IP SIP VR3R3. Please implement them as default values. Filling the below table with customer specific values is only necessary if

- the customer PW Policy is different from the recommended values depicted in chapter xxxx
  and there is no implemented Security Checklist where a PW Policy for the whole Customer scenario is already stated.

The setting of the password policies on the phone for Generic, User and Admin Policy is detailed in the OpenStage / Desk Phone IP Administration manual chapter Security -> Password Policy

	Admin Password	User Password
Minimal Length		
Minimal number of upper case letters		
Minimal number of lower case letters		
Minimal number of numerals		
Minimal number of special characters		
Maximal number of repeated characters		
Change interval		
Maximum number of erroneous login attempts		
Minimum character count for changed characters		
Password History		
Number of days password is kept in history		
Maximum password age in days		
Minimum password age in hours		
Notification before password expiration in days		

	Admin Password	User Password
Maximum number of erroneous login attempts		
Account lockout duration in minutes		
Automatic logoff after not used period in minutes		

6.3 Certificate Handling

Certificates are used to provide authentication of connected servers and Digital keys. Customer generated certificates must be installed on the phone.This section gives a list of the certificates used on the phone.

In addition to installing certificates on the phone,the certificate validation policy must be configured.

There are three levels of checking available:

None	There is no authentication of the server
Trusted	The following is checked • that it is trusted (this means: the chain of trust for the digital signature provided by the remote entity ends up in one of the trusted (e.g. Root CA certificates, which are preconfigured for that interface on the phone) • that it is not expired (i.e. current date/time is within the certificate's given validity period) • that it is not revoked (using OCSP)
Full	It is assumed the server is trusted and there is no need to perform any additional checks. The following checks additional to the “Trusted” policy: • that it has the correct identity (according to settings in altSubjectName and/or the common name (CN) in the Subject) . This may be a FQDN, IPv4 or IPv6 address • that it has the correct use of the following critical extension:OCSP signing.

The CLs for those functions which make use of certificates detail the actions needed to setup up the certificates for that function.

6.3.1 Credentials used for Openstage and Desk Phone IP SIP V3R3

#	Interface	Credential	Customer requirement for OpenStage / Desk Phone IP Phone credentials	Expiration Date for Customer specific key material	Unify Default credentials	Usage
1	HTTPS File Download	Server CA Certificate			None	Remote Server Authentication for file download
2	HTTPS File Download	Phone Client Certificate			None	Mutual Authentication of phone
3	Send URL 1 HTTPS	Server CA Certificate			None	Authentication of remote server for Send URL function 1
4	Send URL 2 HTTPS	Server CA Certificate			None	Authentication of remote server for Send URL function 2
5	Send URL 3 HTTPS	Server CA Certificate			None	Authentication of remote server for Send URL function 3
6	SIP TLS	Server CA Certificate			None	Authentication of remote SIP Server
7	802.1x	802.1xPhone Certificate			None	Authentication of Phone by remote RADIUS Server
8	802.1x	RADIUS Server CA Certificate			None	Authentication of remote RADIUS Server
9	WBM HTTPS	WBM Server Certificate			Unify Default Certificate	Authentication of phone by WEB browser and encryption
	CCE TLS					Same Certificate also used for encryption of CCE interface to OSM and HPT PC applications

#	Interface	Credential	Customer requirement for OpenStage / Desk Phone IP Phone credentials	Expiration Date for Customer specific key material	Unify Default credentials	Usage
10	XML App 1 HTTPS	Server CA Certificate			None	Authentication for XML Application 1. The XML App certificates 1 and 2 can also be used as current and next to allow changeover of certificate for a single server
11	XML App 2 HTTPS	Server CA Certificate			None	Authentication for XML Application 2.The XML App certificates 1 and 2 can also be used as current and next to allow changeover of certificate for a single server
12	OCSP	OSCR 1 Signature CA Certificate			None	Authentication of signature returned from OCSR 1
13	OCSP	OSCR 2 Signature CA Certificate			None	Authentication of signature returned from OCSR 2

6.3.2 Setup Certificate Checking Policy

Table: Certificate Checking

CL-SIP Secure Signalling	
Measures	The level of validation that is done on certificates received by the phone is configurable. The validation levels available are • None • Trusted – only certain aspects of the received certificate are checked • Full – all aspects of the received certificate are checked
References	See Phone Administration Manual chapter on Security -> Certificate Policy
Can be done via	

CL-SIP Secure Signal-ling	
Needed Access Rights	Administrator
Executed Set authentication policy for https secure file trans-fer:	Yes: ☐ No: ☐
Set authentication policy for secure SIP signalling:	Yes: ☐ No: ☐
Set authentication policy for secure Send URL	Yes: ☐ No: ☐
Set authentication policy for 802.1x:?	Yes: ☐ No: ☐
Set authentication policy for XML Applications :	Yes: ☐ No: ☐
Set authentication policy for DLS /WPI	Yes: ☐ No: ☐
Customer Comments and Reasons	

6.4 Port Table

For latest updates of the OpenStage and Desk Phone IP SIP port tables refer to the Interface Management Database (IFMDB) via Unify Partner Portal.

Use the link http://www.unify.com/us/partners/partner-portal.aspx , go to Menu item “support” and then click IFMDB in the pull down menu.

6.5 References

- OpenStage SIP V3R3 administrator documentations (e-Doku or https://www.unify.com/seba/default.aspx Portal / product information)

- VoIP security please
  http://wiki.unify.com/index.php/VoIP_Security
- DLS – Certificate Management for 802.1x / EAP-TLS
  http://wiki.unify.com/images/a/ae/DLS_-_Certificate_Management_for_802_1x.pdf
- OpenStage and Desk Phone IP - Provisioning Interface
  http://wiki.unify.com/images/c/c7/OpenStage_Provisioning_Interface_Developer%27s_Guide.pdf
- Interface Management Database (IFMDB) available via Unify Partner Porta available via SEBA Portal
  https://www.unify.com/seba/default.aspx

Index